DERWENT-ACC-NO: 2000-186780
DERWENT-WEEK: 200018
\~4~COPYRIGHT 1999 DERWENT INFORMATION LTD\~14~
TITLE: Data accessing method using network of radio broadcast, navigation, public notice tower involves using server which authenticates according to authentication demand
INVENTOR-NAME:
PRIORITY-DATA: 1998JP-0198357 (July 14, 1998)
PATENT-FAMILY:

PUB-NO	PUB-DATE	LANGUAGE	PAGES	MAIN-IPC
JP 2000029833 A	January 28, 2000	N/A	005	G06F 015/00

INT-CL_(IPC): G06F015/00; G09C001/00 ; H04L009/32
ABSTRACTED-PUB-NO: JP2000029833A
BASIC-ABSTRACT: NOVELTY - A server (10) transmits required data file based on demand from the terminal equipment and the received data file is stored in a memory (15). An authentication demand of utilization is performed according to which the server apparatus authenticates. When the audit of data utilization performed by authentication (13) is satisfactory, data is utilized in the terminal equipment.

USE - For accessing data using network of CATV, radio broadcast, communication karaoke, TV broadcast, teletext, pager, navigation, game delivery, audio recorder, video recorder, video on demand, public notice tower, etc.

ADVANTAGE - Prevents inaccurate utilization of data and multiple storage of received data. DESCRIPTION OF DRAWING(S) - The figure shows the data accessing method. (10) Server; (13) Authentication; (15) Memory.

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号
特開2000－29833
（P2000－29833A）
(43)公開日　平成12年１月28日(2000.1.28)

(51)Int.Cl.⁷	識別記号	ＦＩ		テーマコード（参考）
Ｇ０６Ｆ　15/00	３３０	Ｇ０６Ｆ　15/00	３３０Ａ	５Ｂ０８５
Ｇ０９Ｃ　1/00	６６０	Ｇ０９Ｃ　1/00	６６０Ｄ	５Ｋ０１３
Ｈ０４Ｌ　9/32		Ｈ０４Ｌ　9/00	６７５Ａ	

審査請求　未請求　請求項の数４　ＯＬ　（全５頁）

(21)出願番号　特願平10－198357

(22)出願日　平成10年７月14日(1998.7.14)

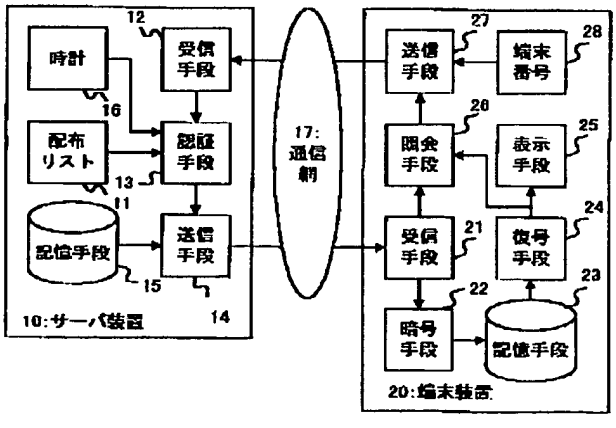
(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地
(72)発明者　亀山　達也
東京都国分寺市東恋ケ窪一丁目280番地
株式会社日立製作所中央研究所内
(74)代理人　100068504
弁理士　小川　勝男

Ｆターム(参考)　5B085 AC03 AC05 AE04 AE23 AE29
BG07
5K013 CA02 CA05

(54)【発明の名称】　データのアクセス方法

(57)【要約】
【課題】ディジタル化されたデータを蓄積・送信するサーバ装置と、ネットワークを経由してデータを受信する端末装置において、受信されたデータを端末装置に複数蓄積し、蓄積されたデータが不正利用されることを防止する。
【解決手段】サーバ装置１０は、端末装置２０からの要求により記憶手段１５に記憶されたデータを記憶手段２３にコピーし、記憶手段２３に記憶されたデータを利用する時、照会手段２６によりサーバ装置１０に問い合わせを行い、認証手段１３によりデータの利用を監査し、問題がなければ、端末装置２０においてデータを利用する。

図１



1

【特許請求の範囲】

【請求項1】データファイルを記憶し要求されたデータファイルを送信するサーバ装置とネットワークを介して接続され、必要なデータファイルをサーバに対して要求し、要求したデータファイルを受信するクライアント装置からなるサーバクライアントシステムにおいて、サーバ装置は、クライアント装置の要求に従って、要求されたデータファイルをクライアント装置に送信し、クライアント装置は、受信されたデータファイルを蓄積する手段により記憶し、受信したデータを利用する場合にサーバ装置に対して利用の認証要求を行い、サーバ装置は、認証要求にしたがって認証を行い、認定要求に対する結果をクライアント装置に通知し、クライアント装置は、結果に応じて、受信したデータファイルを利用することを特徴とするデータのアクセス方法。

【請求項2】請求項1記載のデータのアクセス方法において、クライアント装置は、受信されたデータファイルを暗号化する手段を設け、暗号化されたデータファイルを蓄積する手段により記憶し、データファイルを利用する場合、認証が成功した場合、データファイルの暗号を解き利用することができることを特徴とするデータのアクセス方法。

【請求項3】請求項1記載のデータのアクセス方法において、サーバ装置は、クライアント装置から初めてデータファイルが要求された時、クライアント装置が持つ固有の識別番号とデータファイルの識別番号を配布リストに記憶し、データファイルをクライアント装置に送信し、クライアント装置からデータファイル利用のための認証要求がクライアント装置の識別番号と、データファイルの識別番号とともに受信された場合、それら識別番号とサーバ装置の配布リストに記憶された識別番号と比較し、認証が成功した時、クライアント装置は、データファイルを利用することが可能になることを特徴とするデータのアクセス方法。

【請求項4】請求項1記載のデータのアクセス方法において、サーバ装置は、クライアント装置から初めてデータファイルが要求された時、クライアント装置が持つ固有の識別番号とデータファイルの有効期限を配布リストに記憶し、データファイルに有効期限を追加してクライアント装置に送信し、クライアント装置からデータファイル利用のための認証要求がデータファイルの識別番号とともに受信された場合、サーバ装置の配布リストに記憶されたデータファイルの識別番号に対する有効期限と、サーバ装置が持つ時計手段の日付とを比較し、一致した場合認証が成功し、クライアント装置は、データファイルを利用することが可能になることを特徴とするデータのアクセス方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、複数の人が共有するデータ（例えば文書データやマルチメディアデータ）を記憶するサーバ装置（例えばWWWサーバやデータベースサーバ）と、ネットワーク等を経由して上記データを受信，蓄積または利用（例えば表示）する端末からなるシステム（例えばVOD，通信カラオケ，CATV，TV放送，ラジオ放送，文字放送，ページャ，ナビゲーション，公告塔，ゲーム配信，オーディオレコーダ，ビデオレコーダなど）において、上記データのアクセスを高速化すると同時に上記データの不正利用を防止する機能を有するデータのアクセス方法に関する。

2

【0002】

【従来の技術】インターネットにおいては、WWWサーバにデータを蓄積し、端末のブラウザソフトにより、必要なデータをアクセスし表示しており、同じデータを表示する場合、毎回WWWサーバに要求し同一データを受信していた。また、データの不正利用を防止する方法として、暗号化されたデータを受信し、暗号を解除する場合、暗号の鍵をサーバから入手しデータを利用する方法が知られている。

【0003】例えば米国マイクロソフト（MICROSOFT）社の「WORD」や、同アドビ（ADOBE）社のACROBATなどのアプリケーションソフトでは、これらのソフトウェアで作成された文書データを、パスワード入力によりデータ保護をする仕組みが搭載されている。

【0004】他にデータに有効期限を設け、データを利用するパーソナルコンピュータの持つ時計と比較し、有効期限を超えた場合、データが利用できないようにする仕組みも知られている。

【0005】

【発明が解決しようとする課題】上記の従来の方法では、データが必要な時、毎回サーバ上のデータをアクセスする必要があり、ネットワーク上のトラフィックが多いときは、アクセスに時間がかかることについて考慮されていなかった。また、アクセスの都度パスワードが要求されるものの、一度パスワードを入力すれば、端末の持つ記憶手段にコピーを作成できるような不正利用の問題に対し考慮されていなかった。また、データの暗号を解く鍵をサーバ装置から入手していたため、鍵をネットワーク上で盗まれる可能性がある問題に対し考慮されていなかった。

【0006】データにパスワードを設ける方法では、データのパスワードさえ知っていれば、異なる端末でも、誰でもデータを利用することができる不正利用の問題について考慮されていなかった。そして、上記データに有効期限を設ける方法も、利用するパソコンの内部時計の日付を意図的に変更すれば、無制限に利用できる不正利用の問題について考慮されていなかった。

【0007】本発明の第1の目的は、端末装置がサーバ装置上にあるデータを利用する場合、受信されたデータを端末装置に蓄積することにより、例えばネットワーク

の通信トラフィックが大きい時間を避けられ、データ通信が高速化されたり、蓄積されたデータを再利用することにより通信トラフィックの増加を防止することにある。さらに蓄積されたデータを利用する時、データの利用許可をサーバ装置に問い合わせ、許可された場合のみ、端末装置にコピーされたデータを再利用させることによりデータの不正利用を防止することにある。

【０００８】本発明の第２の目的は、コピーされたデータを端末装置に記憶する時に端末装置が持つ公開されない鍵により暗号化と復号化を行うことにより、データの暗号を不正に解くことを禁止することにある。

【０００９】本発明の第３の目的は、データを利用できる端末を特定することにより、異なる端末でのデータの利用を制限することにある。

【００１０】本発明の第４の目的は、利用可能な有効期限を持つデータの有効期限をサーバ装置上にて確認することにより、端末装置上で日付を変更してデータを利用することを防止することにある。

【００１１】

【課題を解決するための手段】本発明のデータアクセス方法は上記第１の目的を達成するために、端末装置はデータを最初のアクセス時にサーバ装置から一度端末装置が持つ記憶手段に蓄積し、２度目のアクセス時（または毎日または一定期間後の最初のアクセス時）には、端末が持つ記憶手段上のデータにアクセスし、データが不正利用を禁止していた場合、サーバ装置に対してアクセス許可を問い合わせ、サーバ装置は、問い合わせを受けた端末装置でのデータの利用を認証し、問題がなければ端末装置に通知し、端末装置は、該当データの利用を許可する。問題があればデータの利用を禁止もしくはデータを消去する。

【００１２】上記第２の目的を達成するために、サーバ装置からデータを端末装置にコピーする時に、データを端末装置が持つ非公開の鍵を使用して暗号化し、サーバ装置からデータの利用の許可を得た場合のみデータの暗号を解く。また、鍵を利用した暗号化方法の他、独自の圧縮方法など、元のデータと異なるデータ内容に変換する方法も利用できる。

【００１３】上記第３の目的を達成するために、サーバ装置は、端末装置からデータが初めて要求されたとき、要求のあった端末装置の識別番号とデータの識別番号を配布リストに記憶し、データとデータの識別番号を付加して端末装置に送信し、端末装置は受信されたデータとデータの識別番号を記憶手段にて記憶し、端末装置は、データを２度目に利用したい時、端末装置から、利用するデータの識別番号と端末の識別番号をサーバに送信し、サーバ装置は、配布リストの端末装置の識別番号とデータの識別番号とを比較し、一致した場合、端末装置に対し、データの利用を許可し、問題があればデータの利用を禁止するか端末装置にコピーされたデータを消去する。

【００１４】上記第４の目的を達成するために、サーバ装置は端末装置からデータが初めて要求されたとき、データの有効期限とデータの識別番号を配布リストに記憶し、データとデータの識別番号を付加して端末装置に送信し、端末装置は受信されたデータとデータの識別番号を記憶手段にて記憶し、端末装置はデータを２度目以降に利用したい時、端末装置から利用するデータの識別番号をサーバに送信し、サーバ装置は端末装置からデータの利用を問い合わせたデータの識別番号と一致する配布リストのデータの識別番号に対応するデータの有効期限と、サーバ装置が持つ時計とを比較し、該当データが有効期限内であれば、端末装置に対しデータの利用を許可し、問題があればデータの利用を禁止するか端末装置にコピーされたデータを消去する。

【００１５】

【発明の実施の形態】図１は本発明の第１の実施例を示すブロック図、図２は本発明の第１の実施例の配布リストの一例、図３は本発明の第１の実施例のファイル構造の一例である。

【００１６】図１において、１０はサーバ装置であり、送信したファイルの識別番号や送信先の端末の識別番号、ファイルの有効期限を記憶する配布リスト１１，端末装置からの照会要求などを受信する受信手段１２，端末からファイルの利用についての照会を受け付け判断を行う認証手段１３，端末装置にファイルなどを送信する送信手段１４，複数の端末装置に送信するファイルを記憶した記憶手段１５，現在日時を出力する時計１６を有する。

【００１７】２０は端末装置であり、サーバからファイルなどを受信する受信手段２１，受信されたファイルを暗号化する暗号手段２３、暗号化されたファイルを記憶する記憶手段２３，暗号化されたファイルを元に戻す復号手段２４，ファイル内のデータを表示する表示手段２５，ファイルを利用してよいかサーバに問い合わせる照会手段２６，サーバに対し照会信号などを送信する送信手段２７，端末装置ごとに異なる識別番号を持つ端末番号２８を有する。上記サーバ１０と端末２０はＬＡＮや無線通信や公衆回線などの通信網１７によって接続されている。

【００１８】図２において、３０はファイルの識別番号、３１は配布先の端末の識別番号、３２はファイルの有効期限である。また図３において、３３はファイルが認証を必要か識別するための識別子、３４は実際に利用されるデータである。

【００１９】次に図４，図５のフローチャート図に基づいて図１の各部の動作を説明する。本実施例は、ファイル内のデータが文書データであり、端末装置の要求によりサーバが送信したファイルを受信し、ファイル内の文書データを端末装置の表示部分に表示するシステムを例

にとり説明する。もちろん本発明は、ファイル内のデータの種類を制限するものではない。

【００２０】端末装置２０は、初めてファイルの受信を希望する場合（７０）、サーバ装置１０に対しファイル要求とともに端末番号２８を送信し（８２）、サーバ装置１０は、端末装置２０からファイルの受信要求（５０）があった場合、該当するファイルが送信可能か判断（５１）し、送信可能であれば、配付リスト１１に送信するファイルの識別番号をファイル番号３０に、要求を行った端末の端末番号２８を配布先３１に、ファイルの有効期限があれば有効期限を有効期限３２にそれぞれ記録する（５２）。さらに送信するファイルを記憶手段１５から読み出し、ファイルの識別番号３０と認証を必要とする識別子３３を付加（図３）し、要求のあった端末装置２０に送信する（５４）。

【００２１】端末装置２０はファイルが受信された場合（７６）、受信されたファイルを暗号化手段２２にて暗号化（７７）し、蓄積手段２３に記憶する（７８）。同時に蓄積手段２３により蓄積された暗号化されたファイルを復号手段２４により復号（７９）し、表示手段２５により表示（８０）する。

【００２２】サーバの処理５１で送信可能でなければ、送信不可の通知を端末装置２０に対して行い（５３）、端末装置２０は、受信不可の表示（８１）を行う。

【００２３】端末装置２０から２度目以降のファイルの利用が要求された場合、照会手段２６は、サーバ装置に対し、ファイル利用の照会を要求し、同時に利用するファイルの識別番号３０と端末番号２８がサーバ装置１０に送信される（７１）。サーバ装置１０は、照会の要求があった場合（５５）、認証手段１３は、配付リスト１３から該当するファイルの識別番号３０から配布先３１に登録された端末番号と照会要求と同時に、受信された端末装置２０の端末番号２８と比較し(５７)、一致しなければ認証の失敗を端末装置２０に通知（６０）する。一致した場合、次に配布リスト１３の有効期限３２と時計１６を比較（５８）し、有効期限を過ぎた場合、認証の失敗を端末装置２０に通知（６０）する。有効期限内であれば、認証の成功を端末装置２０に通知（５９）する。

【００２４】端末装置２０は、認証の失敗を受信した場合、該当するファイルを消去(７３)する。認証の成功を受信した場合、該当するファイルを復号手段２４により

復号（７４）し、表示手段２５により表示（７５）する。

【００２５】

【発明の効果】本発明によれば、一度サーバ装置にアクセスしたデータを端末の記憶手段に蓄積し、蓄積されたデータの利用許可については、端末からサーバに対しての問い合わせを行うことにより、２回目以降のデータアクセスに対しては、問い合わせに要するデータ量が、蓄積されたデータに比較して極めて小さいため、ネットワークに対する通信負荷が少なく、問い合わせに対するレスポンスも速いため、データ利用を高速化することができる。

【００２６】本発明によれば、受信したデータを端末装置の記憶手段に記憶する時、暗号化して記憶することにより、データの利用をサーバ装置が許可しない限り、記憶されたデータの暗号を解くことができず、不正な利用を防止できる。

【００２７】本発明によれば、サーバ装置に対するデータ利用の問い合わせに、端末が持つ固有の端末番号とデータの識別番号を利用して管理することにより、データを入手した端末装置と異なる他の端末装置でのデータの利用を制限することができる。

【００２８】本発明によれば、データの有効期限の管理において、サーバ装置が持つ時計を基準にデータの有効期限を管理することができるため、端末装置の時間を不正に変更して、データを不正利用することを防止できる。

【図面の簡単な説明】

【図１】本発明の第１の実施例を示すブロック図。

【図２】本発明の第１の実施例の配布リストの一例を示す説明図。

【図３】本発明の第１の実施例のファイル構造の一例を示す説明図。

【図４】本発明の第１の実施例のサーバ装置の動作を示すフロー図。

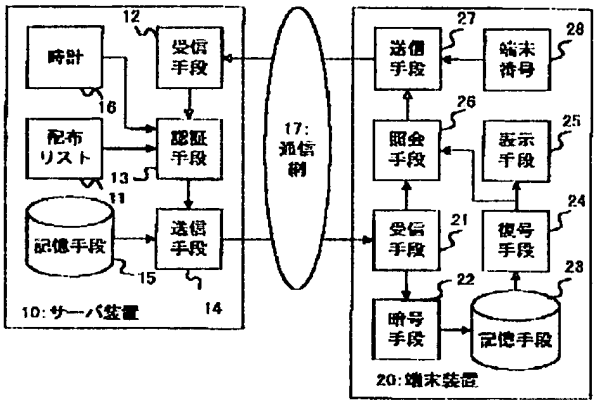
【図５】本発明の第１の実施例の端末装置の動作を示すフロー図。

【符号の説明】

１１…配布リスト、１３…認証手段、１５…記憶手段、１６…時計、２２…暗号手段、２４…復号手段、２６…照会手段、２８…端末番号。

【図1】

図1



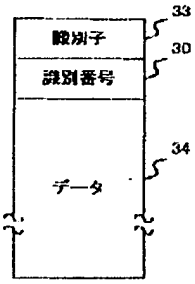
【図2】

図2

30:識別番号	31:配布先	32:有効期限
123456	ABCDEF	98/03/20
2222222	ABCDEF	98/02/20
3333333	ABCDEF	00/00/00

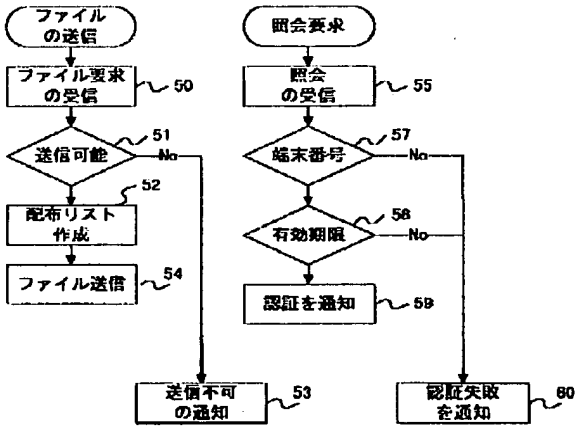
【図3】

図3



【図4】

図4



【図5】

図5